This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

Annex A — Continuous Audit Committee and Compliance of the WCPE

Operational Charter of the Continuous Audit Committee (CAC)

Binding Annex to the Founding Charter of the World Committee for Planet Earth (WCPE)
Master interpretation clause: *In case of conflict or ambiguity, the most restrictive interpretation in favor of the advancement of human life shall prevail.* This rule is hierarchically superior to any other provision of this Annex.

A.0 Preamble

This Annex establishes the **Continuous Audit Committee (CAC)** of the WCPE as a permanent, autonomous, and technically hardened body, charged with verifying **without interruption (24 hours a day, 7 days a week, 365 days a year)** compliance with the Founding Charter, the integrity of validated projects, the traceability of WCPE models, and the detection of any unauthorized use, copy, derivation, or modification of the Committee's cognitive assets — collectively designated as the **Life is Good (LiG) models**.

The CAC operates under the principle of **Absolute Zero Trust** and the doctrine of **Defense in Depth**, assuming that any process, person, organization, or technology can be compromised at any time, including by quantum and post-quantum threats not yet documented.

A.1 Mission, Scope, and Principles

A.1.1 Mission

To ensure continuous, automated, and human verification of compliance with the WCPE Charter — detecting, halting, and sanctioning any deviation, unauthorized use, or alteration of the *Life is Good* models, in any phase (definition, simulation, development, Reduced-APOC testing, implementation, or post-implementation) and in any entity on the planet (project, company, government, NGO, academic consortium, individual).

A.1.2 Scope

The CAC has jurisdiction over:

1. Projects in any phase of the WCPE validation cycle.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

2. Already-implemented projects. **Statute of limitations:** auditing actions for unauthorized use of LiG models lapse 20 years after the date of the act, with interruption upon later discovery of evidence concealed in bad faith. Violations that produce active risk to humanity or the biosphere are **imprescriptible**, in accordance with the principle of international law applicable to crimes against humanity.
3. Every public or private entity that has had partial or total access to a LiG model.
4. Code repositories, package registries, *model hubs*, *datasets*, containers, CI/CD artifacts, *blockchains*, P2P networks, quantum substrates, and any future storage or transmission medium. Platforms named in technical versions of this Annex (Git, npm, PyPI, HuggingFace, Docker, etc.) constitute an **illustrative, non-exhaustive list**, updatable by the CAC without requiring amendment of this Annex.
1. Technical communications (papers, preprints, patents, talks, forums, social networks) where unauthorized disclosure of LiG models is suspected.
2. Specialized hardware (TPU, GPU, QPU, ASIC, FPGA, and successors) that may have executed LiG models.

A.1.3 Operational Principles

#	Principle	Operational Definition
AC-P1	**Absolute continuity**	24/7/365 operation with no simultaneous maintenance windows; multi-continent geographic redundancy.
AC-P2	**Structural independence**	The CAC reports directly to the Gold Team of the Planet (GTP); no audited project may finance, contract, or influence the CAC.
AC-P3	**Absolute Zero Trust**	No member, system, or piece of evidence is presumed valid without multilayer verification.
AC-P4	**Verifiable determinism**	Every sanctioning decision rests on reproducible, signed evidence replicable by independent third parties.
AC-P5	**Reversibility of erroneous decisions**	Mandatory appeal mechanism before the Tribunal of Reversal and Appeal (TRA).
AC-P6	**Inverse proportionality**	For unauthorized use of LiG models, the minimum sanction is full project closure; the CAC does not apply lesser sanctions in this case.
AC-P7	**Anticipatory quantum resistance**	Every cryptographic primitive, hash, signature, and integrity proof is built to resist fully operational quantum adversaries.
AC-P8	**Audit of the auditor**	The CAC itself is audited by a rotating external entity with public disclosure power.
AC-P9	**Delayed radical transparency**	Findings published on the immutable ledger; redaction windows only for active security reasons, capped at 90 days, reviewable.
AC-P10	**Active precaution with due process**	Upon reasonable doubt of unauthorized use, a precautionary, reversible provisional freeze is activated. The initial burden of proof rests on the CAC, which must

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

#	Principle	Operational Definition
		present reproducible *prima facie* evidence; once presented, the audited party bears the burden of producing exculpatory evidence. This articulation preserves due process under the standard of the International Covenants on Human Rights.

A.2 Structure of the Continuous Audit Committee

A.2.1 Human Composition

Seat	Composition	Function
Rotating Auditor General	Designated by the GTP; three-year term, not consecutively renewable	Strategic direction of the CAC
Compliance Committee (5 members)	Specialists in forensic auditing, cybersecurity, international law, ethics, and model engineering	Decision on sanctions
Digital Forensics Team (Blue Forensics)	Analysts in digital chain of custody, reverse engineering, and cryptography	Evidence collection and validation
Audit Red Team	Adversaries contracted by the CAC to attempt to defeat its own detection capabilities	Continuous validation of the CAC
Compliance Purple Team	Blue+Red coordination	Closure of detected gaps
Defender of the Audited Party	Guarantees due process to the investigated party	Protection against false positives
Independent Observers	Three audit firms with no contract with the WCPE	Audit the CAC
Sentinel Node Liaison	Permanent human liaison with the Sentinel AI	Traceability and human supervision

A.2.2 Sentinel Node — Continuous Surveillance Arm

The **Sentinel Node** of the WCPE participates permanently and continuously in the CAC, in accordance with the binding doctrinal clause of the Founding Charter (Section 4.5). Its audit role is operational and technical, **always under human supervision**, without sanctioning vote authority, save for the exceptional case of proven risk to humanity.

A.2.2.1 Continuous Operational Functions of the Sentinel

1. **Surveillance of repositories and substrates:**

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

  - Continuous, automated, and signed monitoring of accessible public and private Git repositories, package registries, *model hubs*, *blockchains*, P2P networks, technical forums, *preprints*, and patents.
  - Search by *fingerprint* of weights, *prompts*, architectures, mathematical derivations, composition hashes, and semantic signatures of LiG models.
  - Detection of *fine-tuning*, distillation, quantization, pruning, knowledge transfer, derived *embeddings*, and any other extraction technique.
2. **Verification of implemented projects:**
  - Periodic re-audit of already-approved projects, without prior notice to the audited party, with updated REP/DRI/HPC metrics.
3. **Behavioral anomaly detection:**
  - Analysis of deployment patterns, latency, energy consumption, and statistical footprints suggesting covert execution of LiG models.
4. **Multi-source correlation:**
  - Cross-evidence among repositories, papers, corporate registries, patents, public telemetry, hardware supply chains, public financial communications, and verified *leaks*.
5. **Generation of technical files:**
  - Every finding is delivered as a signed file to the human Compliance Committee — never as an autonomous decision.

A.2.2.2 Guarantees and Limits of the Sentinel Node in Auditing

- **No access to personal data of the audited party** beyond what is strictly necessary for the finding.
- **No power to execute sanctions**; only delivers evidence.
- **Full traceability of every inference** on the post-quantum ledger.
- **Permanent human veto** over the publication or escalation of any finding.
- **Heterogeneous ensemble of at least three independent models**; a single model does not generate an alert.
- **Deliberative air-gap** in critical investigations.
- **Geographically distributed 3-of-5 multi-party kill-switch.**

A.2.3 Tribunal of Reversal and Appeal (TRA)

- Reinforced quorum to review and, if applicable, reverse sanctioning decisions of the CAC.
- Guarantees due process to the audited party.

A.3 Definition of *Life is Good* (LiG) Models

For the purposes of this Annex, the **Life is Good models** are the set of conceptual frameworks, mathematical formulations, algorithmic architectures, weight sets, curated *datasets*, validation protocols, specific derivations, and any cognitive artifact registered by the WCPE as a planetary asset intended for the equitable advancement of humanity.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

A.3.1 Cryptographic Identity of Each LiG Model

Every LiG model carries: - **Post-quantum master hash** (root identity signature). - **Structural composition hash** (architecture). - **Weight hash** or equivalents for non-neural models. - **Semantic signature** (statistical behavior fingerprint). - **Active watermark** embedded (cryptographic + steganographic). - **Passive watermark** detectable by statistical inference without access to weights. - **Versioned lineage** signed by the International Certifying Authority.

A.3.2 Use Regime

- Free, equitable, and non-monopolizable access, **provided that** prior notification is made to the WCPE and the use case is registered on the immutable ledger.
- Prohibited: commercial, governmental, military, or academic use that **has not been previously registered and authorized**.
- Prohibited: any modification, derivation, distillation, or knowledge transfer that is not declared to the Committee.
- Prohibited: any attempt to evade detection (obfuscatory retraining, architecture change preserving functionality, use of quantum hardware to mask signatures).

A.4 Continuous Audit Processes

A.4.1 Layer 1 — Continuous Passive Surveillance (Always-On)

- Automated monitoring by the Sentinel Node of authorized public and semi-public sources: open repositories, *model hubs*, patent registries, *preprints*, technical forums, public corporate registries, *blockchain explorers*, and public *crash dumps*.
- Frequency: full sweep every 6 hours; continuous *delta scan*.
- Output: signed telemetry to the CAC ledger.

A.4.2 Layer 2 — Scheduled Active Audit

- Mandatory re-audit of approved projects at 30, 90, 365 days, and every 18 months thereafter.
- Inspection of code, infrastructure, data, and processes.
- Negotiated access to the project's private repositories, with independent custodians.

A.4.3 Layer 3 — Suspicion- or Complaint-Based Audit

- Triggered by Sentinel finding, citizen report, protected *whistleblower* alert, external auditor warning, or GTP request.
- Includes forensic investigation, *takedown* coordinated with national authorities, and evidence preservation.

A.4.4 Layer 4 — Continuous Adversarial Audit of the CAC

- The CAC's Red Team attempts weekly to defeat the CAC's own detection processes.
- Results are published on the ledger; any breach is closed before the next window.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

A.4.5 Layer 5 — Anticipatory Quantum Audit

- Monthly testing against simulated adversaries with full quantum capability.
- Continuous migration to post-quantum primitives (Kyber, Dilithium, SPHINCS+, FALCON, and certified successors).
- Replication of the ledger across heterogeneous substrates (classical, quantum-resistant, physically distributed).

A.4.6 Layer 6 — Formal Verification

- Mandatory application of formal verification (Coq, Isabelle, Lean, TLA+, or equivalents) to critical CAC components.
- Annual renewal of formal proofs.

A.5 Detection of Unauthorized Use of LiG Models

A.5.1 Detection Vectors

#	Vector	Technique
D1	**Exact match of weights or code**	Differential hashing, *binary diffing*, *embedding* matching
D2	**Derivation through *fine-tuning***	Statistical proximity-of-function tests; *membership inference*
D3	**Distillation / *teacher-student***	Behavioral analysis under secret *probing prompts*
D4	**Quantization or pruning preserving function**	Structural fingerprints tolerant to transformations
D5	**Re-architecture preserving functionality**	Output *behavioral fingerprint*; *capability probes*
D6	**Active watermark**	Detection of patterns embedded in weights or outputs
D7	**Passive watermark**	Statistical inference without access to weights
D8	**Energy and compute telemetry**	GPU/TPU/QPU load signatures consistent with LiG models
D9	**Side-channel analysis**	Response timing, consumption, *cache traces*
D10	**Paper and patent analysis**	Forensic NLP, search for exclusive mathematical derivations
D11	**Supply chain analysis**	Hardware purchases, quantum compute contracts, technical alliances
D12	**Verified internal reports**	Protected *whistleblowing* channels, multilateral rewards

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

A.5.2 Resistance to Evasion

The CAC assumes that sophisticated adversaries will attempt to render LiG models **undetectable** by modifying them. Mandatory countermeasures:

- **Redundant and heterogeneous watermarks**: if an adversary removes one, the others remain.
- **Secret capability probes**: *prompts* and confidential inputs that a derived model will answer in a characteristic manner, **even after extensive fine-tuning**.
- **Compositional statistical-fingerprint analysis**: internal correlations across layers, gradients, and attention are difficult to erase without destroying the model's utility.
- **Detection of obfuscatory retraining**: measurement of functional divergence vs. expected after *fine-tuning*; anomalous values trigger alerts.
- **Active quantum resistance**: identity hashes are signed with multiple post-quantum primitives; a single broken algorithm does not compromise the system.
- **Zero-knowledge proofs** that the audited party must pass to demonstrate **non-use** of LiG models without revealing sensitive information.
- **Mandatory multilateral cooperation**: signatory states enable access to corporate, fiscal, and compute records under expedited judicial order.

A.6 Sanctioning Regime

A.6.1 Finding of Unauthorized Use of a LiG Model (Minimum Sanction)

When the CAC determines, with reproducible evidence and due process, that a project, company, government, association, consortium, or person has **used, copied, derived, or modified** a LiG model without WCPE authorization or prior notification, the following **minimum and indivisible sanction** shall apply:

1. **Immediate and complete closure of the project** associated with the unauthorized use, defined as full suspension of technical, commercial, and dissemination operations linked to the misuse.
2. **Cessation of operations** of the business, company, association, organization, or consortium that participated in the development, commercialization, or deployment. Execution of this point requires cooperation with the competent national jurisdiction under the founding Treaty. In non-signatory jurisdictions, the WCPE activates indirect measures (Section A.6.6).
3. **Planetary disqualification** for at least 25 years from participating in WCPE-validated projects, including the entity's supply chain and entities linked by shareholding or direct control.
4. **Verifiable confiscation and destruction** of derived artifacts (weights, data, code, contaminated specialized hardware), executed by national authorities with the CAC as technical observer, under signed chain of custody.
5. **Full publication** of the file on the CAC's immutable ledger, with minimum redaction only for non-essential personal data.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

6. **Notification to signatory states** for activation of applicable national legal frameworks.
7. **Mandatory reparation** through a contribution equivalent to the calculated damage paid into planetary public-goods funds.

A.6.2 Aggravating Factors

- Military or coercive use: closure extended to the entity's entire productive apparatus and lifetime ban on responsible individuals.
- Attempt at evasion, modification, or obfuscation aimed at undetectability: automatic aggravator that doubles the disqualification period.
- Use of quantum technology to mask signatures: aggravator equivalent to the prior point.
- Recidivism: permanent planetary disqualification.

A.6.3 Mitigating Factors

- Self-disclosure prior to the start of the audit, with full cooperation.
- Voluntary notification of accidental derivation.

A.6.4 Due Process

- The audited party has the right to a documented reply before the sanctioning decision, with a minimum period of 30 working days from notification.
- The Defender of the Audited Party guarantees access to evidence, free legal assistance, and translation where applicable.
- Appeal before the TRA with reinforced quorum (7 of 9), with a maximum resolution period of 180 calendar days, extendable by 90 days by unanimity.
- **Maximum total period of the procedure (admission to final ruling):** 12 months, save for an exceptional, motivated, and published extension.
- **Execution of the sanction:** the final sanction is executed after exhaustion of the appeal. While the procedure is pending, only the precautionary provisional freeze (AC-P10) operates — reversible and not entailing destruction of assets. Excepted is the case of active risk to humanity, in which the GTP may authorize provisional execution with expedited TRA review within 30 days and reparation in the event of confirmed error.

A.6.5 Master Clause Applied

In case of conflict or ambiguity over the application of sanctions, the most restrictive interpretation in favor of the advancement of human life prevails — understanding that the integrity of LiG models is a planetary public good and that their unauthorized use erodes the equitable advancement of humanity.

A.6.6 Enforcement Against Entities in Non-Signatory Jurisdictions

When a violation originates in a non-signatory state or one whose jurisdiction does not cooperate, the CAC executes:

1. **Public registration** in the World Registry of Non-Compliant Entities.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

2. **Collateral restrictions** agreed with signatory states: prohibition on contracting with the entity, exclusion from public procurement, restriction on transfer of specialized hardware, denial of access to academic networks and multilateral funding.
3. **Severance of interoperability** with WCPE scientific and technical infrastructure.
4. **Active diplomacy** with the host state to incentivize Treaty accession.
5. **International litigation** before tribunals of universal competence when the case constitutes a crime against humanity.

A.6.7 Audited Party's Refusal of Access

Refusal, obstruction, or untimely delivery of information required under expedited judicial order constitutes an **automatic infraction equivalent to unauthorized use** and triggers the minimum sanction of A.6.1, without prejudice to national contempt sanctions.

A.6.8 Personal Data Protection

The CAC's actions respect applicable personal data protection standards (including, without limitation, the principles of the GDPR, the Council of Europe's Convention 108+, and equivalent norms). Personal data are processed under principles of minimization, specific purpose, limited retention, and data-subject rights, without compromising the evidentiary value of the audit.

A.7 Failure Resistance and Adversary Tolerance

A.7.1 Tolerance to Technical Failures

- Geographic redundancy of the CAC across at least five continents.
- Replication of the ledger across at least seven independent substrates. Three (classical, post-quantum, physically distributed) are **production substrates** with service guarantee. The remainder (optical, magnetic, biological-DNA, experimental-holographic) operate as **experimental substrates** with cumulative evidentiary value, validated by independent third parties before being admitted as primary evidence.
- Automatic *failover* in less than 60 seconds.
- Quarterly disaster recovery (DRP) and business continuity (BCP) testing.

A.7.2 Tolerance to Human Adversaries

- Mandatory personnel rotation with prepared succession.
- Compartmentalization of information (need-to-know).
- Selective anonymity in critical decisions.
- Jurisdictional refuge for investigators under threat.
- Protection for *whistleblowers* with shielded identity and multilateral compensation.

A.7.3 Tolerance to Quantum Adversaries

- Pre-quantum migration completed before the estimated horizon of relevant quantum compute.
- Multiplicity of primitives: if one is broken, the others sustain the system.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- Multiple signatures per event, with at least three distinct mathematical families.
- Detection of retroactive decryption (*harvest now, decrypt later*) through signed decoys with verifiable timestamps.

A.7.4 Tolerance to Manipulation of the CAC Itself

- Annual rotating external audit.
- Publication on ledger of every internal decision.
- Direct citizen reporting channel to the GTP.
- Immediate disqualification of any CAC member with detected conflict of interest.

A.7.5 Tolerance to False Positives and False Negatives

- Mandatory double evidence before any final sanction.
- Control tests using certified benign datasets for continuous Sentinel calibration.
- Public metric: false-positive and false-negative rates of the CAC, externally audited.

A.7.6 Digital Chain of Custody

- All collected evidence is cryptographically signed at the moment of capture with a verifiable timestamp and an automated independent witness.
- The chain of custody is replicated across at least three ledger substrates before being used in proceedings.
- Any break in the chain of custody invalidates the evidence and requires fresh collection.

A.7.7 Inter-Jurisdictional Coordination of the CAC

- When a case involves several jurisdictions, the CAC designates a coordinating cell with representation from the affected regions.
- Decisions are taken by internal consensus; in case of disagreement, the matter escalates to the GTP.
- Operational actions in the territory of a state are executed exclusively in cooperation with its competent national authority.

A.8 Compliance Metrics

Metric	Definition	Target
CC-01 Monitoring coverage	% of registered sources continuously monitored	≥ 99.5% monthly
CC-02 Detection latency	Time from public appearance of a derivation to Sentinel alert	≤ 24 hours for open sources
CC-03 False positives	Findings refuted after due process	≤ 0.5% annually
CC-04 Detected false negatives	Late detections by *whistleblower* or external audit	≤ 0.1% annually with continuous-improvement objective
CC-05 Sanctioning	From final ruling to	≤ 72 hours

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

Metric	Definition	Target
closure time	operational closure of the audited party	
CC-06 Post-quantum coverage	% of system primitives with post-quantum resistance	100%
CC-07 CAC availability	Aggregate uptime	≥ 99.999%
CC-08 Internal Red Team success rate	% of evasion attempts that succeed against the CAC	≤ 1%, with mandatory closure in the next window
CC-09 Audit of the auditor	External observer findings closed on schedule	100%

A.9 Integration with the WCPE

- The CAC reports daily to the GTP via encrypted dashboard.
- Every sanction first clears the Compliance Committee filter; global decisions of systemic impact require GTP ratification with 3/5 quorum + Sentinel non-veto + defenders' non-veto.
- The Sentinel Node operates under the binding doctrinal clause of Section 4.5 of the Founding Charter: advisory voice by default, exceptional vote only under proven risk to humanity and in accordance with the Extended Asimov Directives.
- CAC decisions are recorded on the WCPE's global immutable ledger.
- The CAC publishes a quarterly Planetary Compliance Report, translated into the Committee's official languages.

A.10 Final Clauses

1. This Annex is an integral and binding part of the WCPE Founding Charter.
2. Any modification requires 4/5 GTP quorum, defenders' non-veto, and a minimum 90-day public consultation.
3. In case of conflict or ambiguity, **the most restrictive interpretation in favor of the advancement of human life prevails**.
4. The continuous operation of the CAC is a *sine qua non* condition for the legitimacy of any global deployment validated by the WCPE.

Annex A.1 — Abbreviated CAC Glossary

- **CAC:** Continuous Audit Committee.
- **LiG:** *Life is Good*, designation of WCPE models.
- **REP / DRI / HPC:** integrated metrics for risk, damage, and public trust footprint.
- **Active / passive watermark:** identification mechanisms embedded and detectable with or without access to weights.
- **Membership inference:** technique to determine whether a datum or model is derived from another.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- **Harvest now, decrypt later:** adversarial strategy of capturing encrypted data for future quantum decryption.
- **Zero-knowledge proof:** cryptographic proof demonstrating a claim without revealing sensitive information.
- **TRA:** Tribunal of Reversal and Appeal.
- **GTP:** Gold Team of the Planet.

LICENSE AND CONDITIONS OF USE.
The content is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license:
https://creativecommons.org/licenses/by-nc-sa/4.0/
By using this content and model, you agree to:
Provide appropriate credit, include a link to the above license, and indicate if changes were made.
Not use the material or any derivative works for commercial purposes.
Distribute any adaptations or derivative works only under the same CC BY-NC-SA 4.0 license.
Not apply legal terms or technological measures that legally restrict others from doing anything the license permits.
Data logging and trade secrets policy.
The design, implementation, and deployment of this model, as well as any derivatives, do not authorize the collection, storage, or exploitation of IP addresses, unique device identifiers, or other technical traceability data for commercial profiling, targeted advertising, or any other economic exploitation.
Any system implementing this model must limit the logging and retention of IP addresses and other identifiable data strictly to what is necessary to:
(a) maintain technical security and service integrity; and
(b) comply with applicable legal obligations (for example, any minimum log retention required by law).
It is prohibited to use this model or its derivatives to:
capture, store, or exploit trade secrets, proprietary know-how, or confidential information of users or third parties for any purpose other than providing the technical service described in this documentation; or train or improve closed, commercial systems using data that contains confidential information of third parties without their prior, explicit, written consent.

---+EOD+---